



KING COUNTY
IT SECURITY ANALYST
SENIOR SYSTEMS ENGINEER
OFFICE OF INFORMATION RESOURCE MANAGEMENT
Annual Salary Range: \$59,575 - \$88,190
Job Announcement: 06CY5983
OPEN: 4/3/06 CLOSE: Open until Filled

WHO MAY APPLY: This career service position is open to the general public.

WHERE TO APPLY: Required application materials can be mailed to: **Terra Strouhal, 701 Fifth Avenue, Suite 3460, Seattle, WA 98104. Fax (206) 205-0725.** Email applications are encouraged at oirmrecruit@metrokc.gov (all application materials must be included). PLEASE NOTE: Applications not received at the locations specified above and those that are not complete may not be processed.

FORMS AND MATERIALS REQUIRED:

- King County application form. Application forms may be found at <http://www.metrokc.gov/ohrm/jobs/JobApplications.htm>
- Resume
- A letter of interest not to exceed two pages in length detailing your background and describing how you meet or exceed the requirements.

WORK LOCATION: 700 Fifth Ave, Seattle Municipal Tower, Seattle, WA.

WORK SCHEDULE: This position is exempt from the provisions of the Fair Labor Standards Act, and is not overtime eligible. The workweek is normally Monday through Friday 8:00 a.m. to 5:00 p.m.

POSITION PURPOSE: This position will report to the county's Chief Information Security/Privacy Officer (CISPO) and will assist in developing and maintaining the county's information and security privacy program. The Security Analyst's role is to identify and resolve potential security breaches and vulnerability issues in a timely and accurate fashion. This person will also ensure the secure operation of the organization's information security systems, servers, and network connections. This position will work with other staff to determine security needs, develop, implement and maintain solutions, and create and enforce security policies.

PRIMARY JOB DUTIES INCLUDE:

- Proactively protect the integrity, confidentiality, and availability of information technology resources by:
 - Responding in a timely manner to a loss or misuse of information technology assets
 - Participating in investigations of suspected information technology security misuse or in compliance reviews as requested by auditors.
 - Communicating unresolved information technology security exposures, misuse, or noncompliance situations with the CISPO and other appropriate management.
- Monitor VPNs, server logs, firewall logs, intrusion detection/prevention logs, network traffic and other security systems for unusual or suspicious activity. Interpret activity and implement plans for resolution.
- Work with the Network Engineering, Network Operations and other groups to manage connection security for local area networks, wide area networks, Web sites, intranets/extranets/portals, and e-mail communications.

- Plan, design, and implement security systems and their corresponding or associated software, including firewalls, VPNs, intrusion detection/prevention systems, cryptographic systems, biometrics, anti-malware vulnerability management and patch management software.
- Work with CISPO and other staff to develop and oversee enforcement of IT security policies and procedures.
- Design, perform, and/or oversee penetration tests to identify system vulnerabilities.
- Assist in designing and implementing disaster recovery plans.
- Conduct research on emerging products, services, protocols, and standards.
- Recommend and deploy additional security products and tools, or enhancements to existing tools, to detect violations of network security measures.
- Other duties as assigned.

QUALIFICATIONS:

- Four years of experience directly related to information technology security. This experience should include active participation in security programs and processes that have contributed to the development and administration of an organization wide IT security architecture.
- Bachelor's degree in Computer Science, Engineering, Business, or related discipline is desired.
- Demonstrated experience with network and IT security components, including firewalls, intrusion detection systems, anti-malware software, data encryption, VPN's, vulnerability scanners, server operating systems, and other industry-standard techniques and practices.
- Knowledge of TCP/IP, and other network protocols, including their vulnerabilities and solutions.
- Working technical knowledge of current systems software, operating systems, and PC protocols and standards.
- Knowledge of applicable laws and practices relating to information privacy and security.
- The demonstrated ability to apply analytical and problem-solving skills to information security and privacy issues.
- Ability to conduct research into security issues and products as required.
- Ability to effectively communicate both verbally and in writing to both technical and non-technical staff on issues of information security. The ability to write documents ranging from formal and informal reports, system documentation, and training materials. Must be able to prepare these materials with limited advance notice.
- The ability to work with limited supervision and limited direction.
- The demonstrated ability to work effectively in a collaborative team environment.
- The ability to prioritize and execute tasks in crisis situation.
- The demonstrated ability to apply effective organizational skills and excellent attention to detail.

LICENCES/CERTIFICATION REQUIREMENTS:

- SSCP, GIAC or equivalent is highly desirable.
- CISSP, CISM, CISA are preferred.
- Training on ISO 17799, COBIT and/or NIST standards is preferred.

NECESSARY SPECIAL REQUIREMENTS: Selected candidate must pass a background investigation as a condition of employment.

SELECTION PROCESS: Applications will be screened for qualifications. Competitive applicants will be invited to an interview. Finalists may be asked to complete a post interview research exercise. Salary will depend on qualifications.

UNION REPRESENTATION: This position is represented the International Federation of Professional and Technical Engineers L17 Information Technology bargaining unit.

CLASS CODE: 732802